

雲端電子郵件安全性 (CES)

Cloudflare 是分析師公認的電子郵件安全領導者，
可預先偵測並阻止網路釣魚威脅

防禦針對性網路釣魚攻擊

輕鬆封鎖或隔離其他解決方案遺漏的威脅

由於電子郵件是人們最常使用且最常利用的商業應用程式，因此，保護使用者免受試圖操縱其信任的網路釣魚攻擊比以往任何時候都更為重要。由於組織越來越多地透過 Microsoft 365 和 Google Workspace 來採用雲端電子郵件服務，以更好地支援混合工作人員，威脅執行者已轉向更具針對性的低流量攻擊，這些攻擊能夠規避如 Proofpoint 和 Mimecast 等傳統的安全電子郵件閘道 (SEG)。

正因為如此，Cloudflare 的雲端原生電子郵件安全解決方案（稱為 Area 1）經過獨特設計，能夠善用先發制人的活動情報、以 ML 為基礎的內容分析，以及統一的 Zero Trust 平台來阻止網路釣魚威脅您的員工。

91%

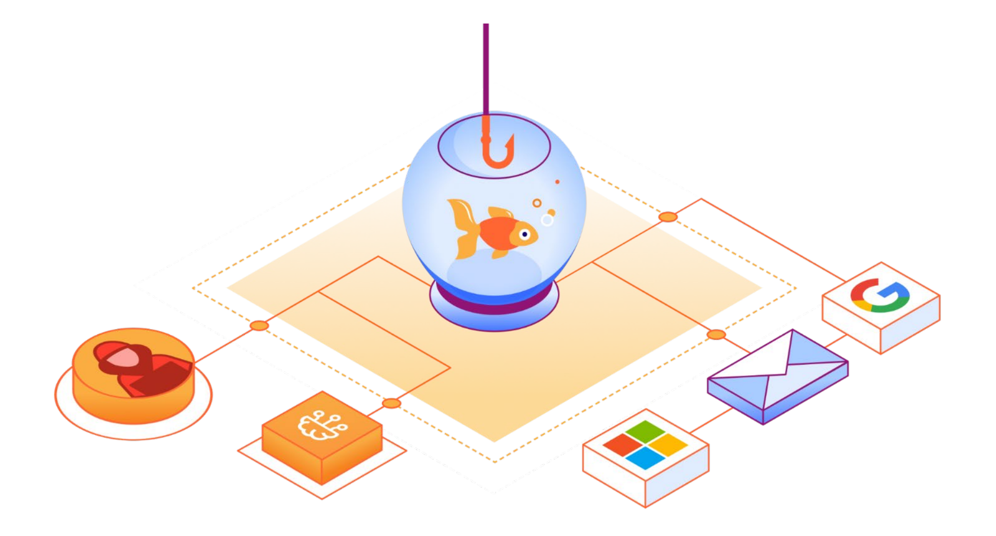
的網路攻擊從網路釣魚電子郵件開始[1]

500 億

這是過去十年的 BEC 攻擊損失[2]

81%

的組織在過去 12 個月內經歷了一起多通道攻擊[3]





阻止商業電子郵件入侵 (BEC)

使用分層且採用 ML 技術的關聯式分析來偵測被冒充和遭入侵的帳戶。



隔離延遲和多通道攻擊

讓使用者免受透過未知或詐騙性連結傳遞的惡意 Web 內容影響。



封鎖勒索軟體和惡意附件

防止勒索行為和惡意程式碼破壞您的組織。

更強的保護性和簡便性

實作分層網路安全，從而以較低的成本提供更強的保護

隨著網路釣魚攻擊的不斷激增，Microsoft 和 Google 繼續擴建原生功能，以支援基本的電子郵件和資料保護功能，例如，驗證、封存、資料丟失預防 (DLP) 和用戶端加密。然而，威脅執行者卻改進了策略來執行更具針對性的規避性攻擊，這些攻擊往往可以繞過原生網路安全控制，從而提高成功率。

藉由在 Cloudflare 上分層，組織可以自動封鎖或隔離針對性網路釣魚攻擊，這些攻擊利用惡意連結、附件和遭入侵的帳戶來竊取敏感性資訊和實施金融詐騙。

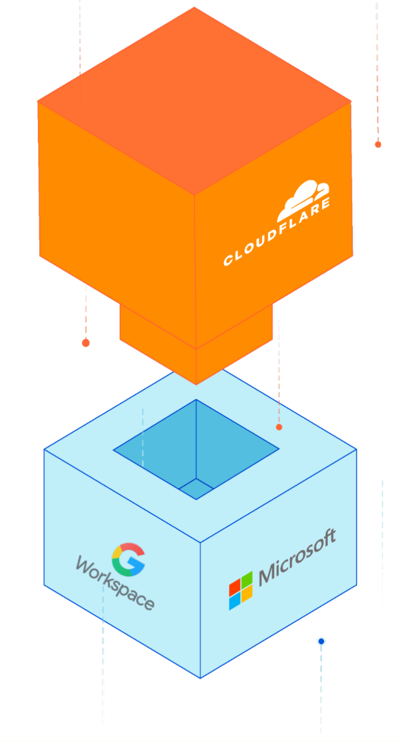
擴充現有的輸入安全控制

Cloudflare 的雲端原生電子郵件安全解決方案可以在幾分鐘內完成部署，以增強現有的 SEG 部署或額外增強 Microsoft 和 Google 提供的內建電子郵件功能。幾乎無需調整，組織便能夠實現更強的網路釣魚保護，同時減少在持續解決方案管理上投入的時間和精力。

「自 [在 M365 上] 實作 Cloudflare 以來，我們的使用者每天收到的惡意或可疑電子郵件數量減少了 50%。這就為我們騰出了好幾個小時的時間，可以重新投資其他目標。」

Werner Enterprises
（財富 1,000 強公司）





電子郵件提供者：
基本的電子郵件和
資料功能



重新投入因自動化程度提高而省下來的時間

Cloudflare 的自動化輕量級解決方案可與 Microsoft 和 Google 工作流程無縫整合，同時為分析師活動提供單一而直覺化的 UI。



偵測功效達到 99.997%

將電子郵件提供者的原生功能與 Cloudflare 的網路釣魚和 BEC 保護相結合，可確保企業擁有全面的覆蓋範圍，從而將風險降至最低。



以更低的成本實現更大的價值

用 Cloudflare 的低觸控解決方案取代過時、昂貴且複雜的部署，可降低營運開銷、備援功能以及過度調整。

阻止複雜的 BEC 攻擊

報告損失達 500 億美元並在不斷增長

在過去十年中，BEC 攻擊造成了驚人的經濟損失，而令人吃驚的是，一些組織仍然沒有優先處理這種有效的金融詐騙形式。雖然 BEC 攻擊在網路釣魚威脅中所佔的比例要小得多，但 SEG 和雲端電子郵件提供者往往不會發現這類攻擊，從而導致更大的財務損失。這些有針對性的攻擊很難發現，因為它們會利用被冒充或遭入侵的帳戶和對話環境來偽裝成員工或受信任的廠商。

將 Zero Trust 原則延伸至電子郵件

當利用遭入侵的員工或廠商電子郵件帳戶時，攻擊者可以規避傳統的安全控制，這些控制僅會嘗試確認傳送者帳戶的合法性。Cloudflare 會進一步分析大量的行為屬性、書寫模式、情緒指標和交談歷史，以確定傳送者的真實性。Cloudflare 的 ML 支援的威脅模型和廣泛的網路情報提供了最有效的武器，可以抵禦用來獲取詐騙性付款的遭入侵帳戶。



圖 1： 郵件分析

使用以 ML 為基礎的關聯式分析來偵測 BEC

準確識別 BEC 攻擊不僅需要對郵件進行結構分析。成功偵測還需要精細理解對話風格和意圖的變化。Cloudflare 龐大的網路遙測（每天超過 1T 的 DNS 要求）和不斷演進的 ML 模型為小型模式分析引擎提供支援，該引擎會解構電子郵件的所有方面來評估書寫模式、情緒、歷史背景以及大量的其他變數，幫助發現傳送者的真實性。

隔離危險的和詐騙性 URL

保護使用者遠離不受信任的電子郵件連結

隨著現代網路釣魚攻擊的欺騙性越來越強，即便是訓練有素的安全解決方案也難以確保 100% 準確識別惡意連結。縮短連結會透過支援延遲攻擊來加劇此問題，因為在延遲攻擊中，會在傳遞後啟用惡意連結。這會導致增加：

- **風險**（因為點擊未知連結）。
- **中斷**（可能會封鎖安全連結）。
- **成本**（因為調查不受信任的連結）。

使用調適型隔離，Cloudflare 消除了惡意軟體和其他惡意 Web 內容，讓使用者能夠安全存取不受信任的連結，從而避免了耗時的調查和原則更新工作。

防止多通道網路釣魚攻擊

雖然電子郵件仍然是惡意連結的主要傳遞機制，但攻擊者已經擴大了攻擊策略，不僅僅限於電子郵件，還在用於日常協作的各種應用程式中攻擊使用者。透過使用 Cloudflare 的 Zero Trust 平台將保護擴展到電子郵件以外，組織可以主動讓使用者免受來自以下應用程式之惡意 Web 內容的影響：











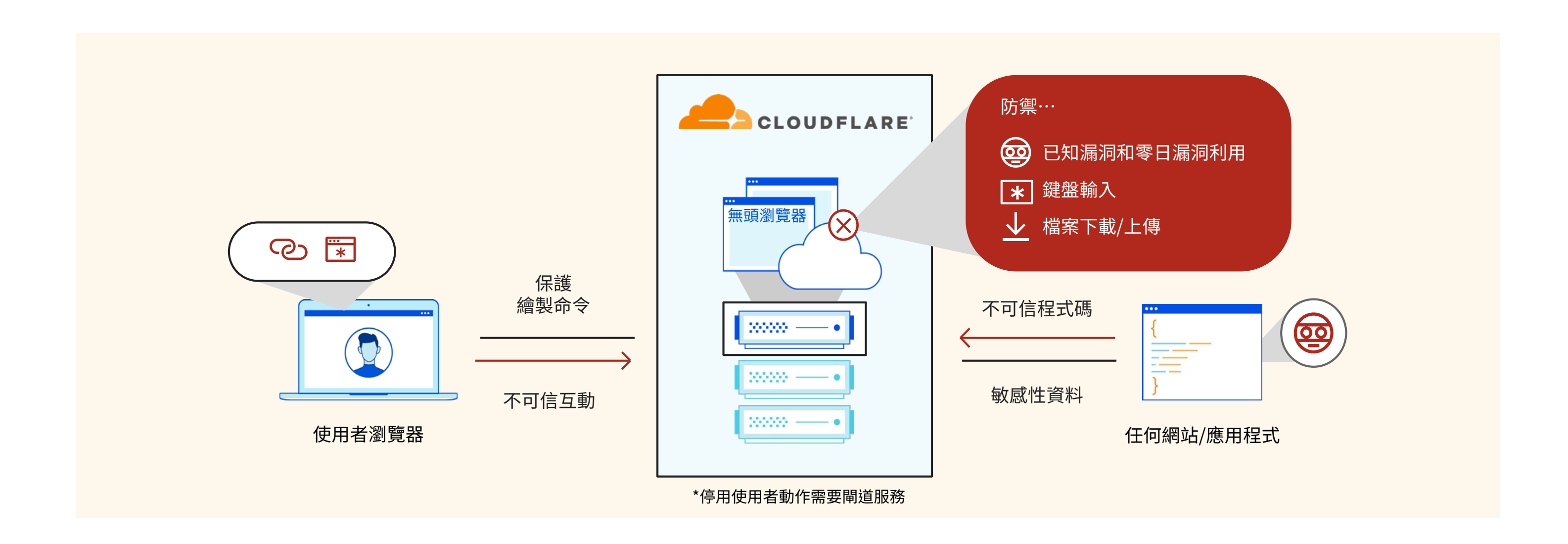



圖 2： 隔離的工作階段

重塑遠端瀏覽器隔離安全

Cloudflare Browser Isolation 使用專屬的網路向量渲染 (NVR) 技術提供無縫、安全且可擴展的解決方案，來隔離不受信任的連結和 Web 內容。NVR 可將安全的輕量級繪製命令串流至裝置，並且隔離的瀏覽器工作階段能夠在 Cloudflare 網路所覆蓋的 300 多座城市的任意資料中心內的任意伺服器上執行。這有助於消除不受信任的程式碼在終端使用者裝置上執行的風險，同時提供使用者看不到的透明的低延遲體驗。

快速調查與回應

直覺化的低觸控解決方案管理

憑藉更高的自動化程度以及獲得最佳結果所需的最低設定，Cloudflare 顯著減少了持續電子郵件安全管理所需的時間和精力。網路安全團隊可以立即完整檢視儀表板中的所有主要指標和趨勢，並且只需按一下，即可瞭解已標記郵件的更精細的詳細資料。透過深入剖析趨勢，可以快速發現頻繁的攻擊類型、成為攻擊目標的高管、已緩解的延遲攻擊以及其他關鍵資料點。

所有分析、遙測、值得注意的威脅以及入侵指標 (IOC) 都可以透過廣泛的 API 提供，以便輕鬆整合到現有的分析工作流程和協調工具中。

「我經常跟同事說，使用 Cloudflare 作為雲端 Saas 解決方案非常簡單輕鬆，而且我對它的高度準確性極為滿意。」

日本航空

受管網路釣魚偵測和回應

Cloudflare 的受管電子郵件安全服務 PhishGuard 可補充您現有的 SOC 團隊，以騰出安全調查週期，並提供有價值的威脅情報。PhishGuard 可透過協助調查、內部人員威脅評估、主動打擊欺詐以及複雜的補救需求，幫助消除網路釣魚活動。PhishGuard 擴展了網路安全資源和專業知識，可以主動通知潛在的欺詐和內部人員威脅，同時還可以執行基於電子郵件的威脅搜尋。

PhishGuard 功能和優點：

- 受管網路釣魚提交和事件回應，以加快解決問題。
- 主動式 BEC 和詐騙通知，讓組織可以在攻擊生命週期早期快速回應。
- 用於即時監控、定期帳戶審查以及持續威脅評估的專用資源。
- 基於對受管環境的威脅分析的自訂封鎖簽章。

1100+

小時，這是實現手動分流工作自動化後每年節省的時間

Cloudflare 的自動化解決方案可消除耗時的手動工作，從而縮短了回應時間並釋放了額外的週期。

50%

傳遞的惡意或可疑電子郵件得以減少（在 M365 上）

在 Microsoft 365 上分層 Cloudflare 讓組織能夠發現針對性攻擊，並減少惡意電子郵件總數。

40

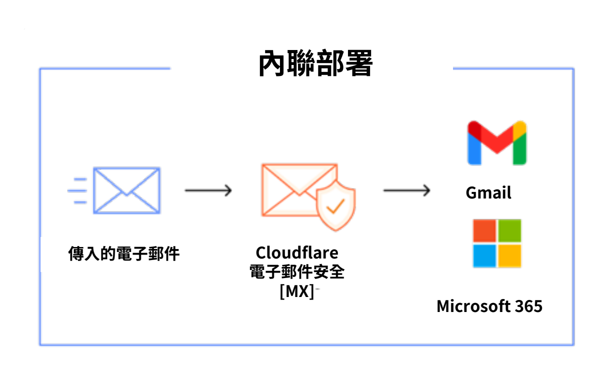
小時，這是七年來在電子郵件安全設定上花費的總時間

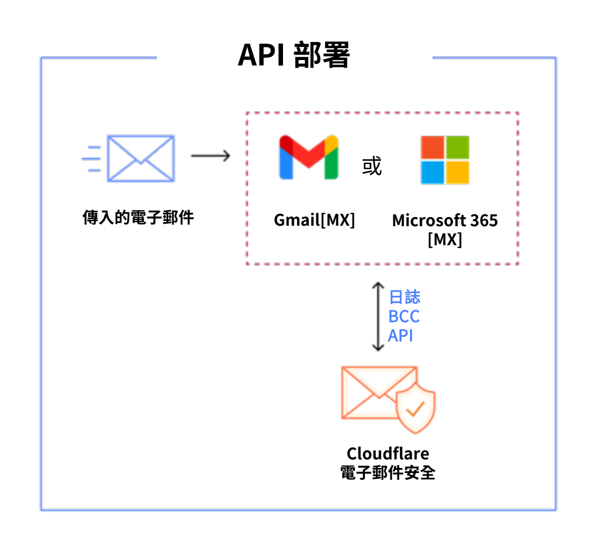
Cloudflare 的低觸控電子郵件安全幾乎無需前期設定和持續調整，可提供開箱即用的高偵測功效。

靈活且易於部署的保護

內嵌、API 和多重模式選項，可實現快速、簡單的部署且不會增加風險

組織可以選擇最適合其環境的方法並在幾分鐘內完成部署，且無需任何硬體、代理或設備。與 SEG 或僅限 API 的廠商不同，Cloudflare 提供靈活的選項，可支援傳遞前和傳遞後保護來進行持續的威脅補救，同時提供與現有 SOC 工作流程以及 SIEM/SOAR 平台的無縫整合。





FORRESTER 2023 年第二季 Forrester Wave™
企業電子郵件安全領導者

評估與比較

啟動網路釣魚風險評估 (PRA)，看看遺漏了哪些攻擊

快速評估電子郵件環境，確定哪些網路釣魚威脅僥倖逃過了目前的防禦。與其他開箱即用的零調整提供者進行比較，看看哪款電子郵件安全解決方案可提供最快速且最簡單的保護。

立即體驗市場領先的網路釣魚保護

申請 PRA

1. 2020 年 Deloitte 研究：來源
2. 2023 年 FBI IC3 PSA：來源
3. 2023 年 Forrester 商機快照：來源